AMENDMENTS TO THE CLAIMS

Applicant submits below a complete listing of the current claims, including marked-up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing. This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple identities each with an associated display name, comprising:

(a) on a first graphic user interface, displaying a name conflict indicator next to a first ~~and a second~~ display name~~, which display names are~~ that is associated with a first identity, the first identity being different than at least one second identity associated with at least one second display name, the at least one second display name being ~~identities and are~~ equivalent to the first display name;

(b) in response to user input associated ~~a selection of a display name~~ with ~~a~~ the name conflict indicator~~displayed next thereto~~, displaying ~~all~~ a plurality of display names that are equivalent to the ~~selected~~ first display name; ~~and~~

(c) ~~providing a mechanism to resolve the name conflict between two conflicting display names~~ receiving user input specifying an alternative display name for a selected display name of the plurality of equivalent display names, the selected display name being associated with a selected identity and being different than the first display name; and

(d) identifying on a second graphic user interface the selected identity with the alternative display name, the graphic user interface providing a function related to controlling communication within the peer-to-peer collaboration system.

2. (Original) The method of claim 1 wherein step (a) comprises computing a clean name from each display name and comparing clean names of two display names to determine if the two display names are equivalent.

3. (Original) The method of claim 1 wherein each contact identity has an authentication level associated therewith and wherein step (a) comprises:

(a1) examining the authentication levels of all display names that are equivalent; and

(a2) displaying name conflict indicators next to selected display names based on the examination in step (a1).

4. (Original) The method of claim 3 wherein step (a2) comprises displaying a name conflict indicator next to each display name associated with a contact identity whose authentication level (1) is less than the highest authentication/certification level of all contact identities with equivalent display names or (2) equals the highest authentication/certification level to which at least two contact identities with equivalent display names have equal authentication levels.

5. (Currently Amended) The method of claim 3 further comprising:

~~(d)~~(e) ~~providing a security policy that determines~~ determining the behavior of the collaboration system regarding communications with a contact based on a security policy and the authentication level of that contact.

6. (Currently Amended) The method of claim 5 ~~wherein step (d) comprises allowing~~ further comprising:

(f) receiving from a user of the collaboration system input specifying ~~to determine~~ the security policy.

7. (Currently Amended) The method of claim 5 ~~wherein step (d) comprises allowing~~ further comprising:

(f) receiving from a system administrator input specifying ~~to determine~~ the security policy.

8. (Currently Amended) The method of claim 5 further comprising:

~~(e)~~(f) warning a user based on the security policy when that user attempts to communicate with a contact having a predetermined authentication level.

9. (Currently Amended) The method of claim 5 further comprising:

~~(e)~~(f) preventing a user from communicating with another user based on the security policy when the other user has a predetermined authentication level.

10. (Currently Amended) The method of claim 1 wherein step (b) comprises displaying a dialog box having all display names that are equivalent to the ~~selected~~ first display name listed therein.

11. (Currently Amended) The method of claim 1 wherein step (c) comprises assigning the alternative display name as an alias to ~~one of~~ the ~~first and second~~ selected display ~~names~~ name which alias is not equivalent to either of the first and second display names and which alias replaces the ~~one~~ selected display name.

12. (Currently Amended) The method of claim 1 further comprising:

~~(d)~~(e) displaying an authentication indicator next to a display name that is not equivalent to another display name, which authentication indicator displays the authentication level of the associated contact.

13. (Original) The method of claim 12 wherein each contact can have one of a predetermined number of authentication levels and wherein the authentication indicator that is displayed is unique to one of the authentication levels.

14. (Currently Amended) A method for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple authentication and certification levels, including an unauthenticated and uncertified level, comprising:

(a) setting a security policy that controls the behavior of the collaboration system based on the authentication and certification level;

(b) receiving through a graphic user interface an indication of a selected contact with which to communicate;

~~(b)~~(c) obtaining the authentication and certification level of the selected contact; ~~in response to an attempt by a user to communicate with one or more contacts, compiling a list of unauthenticated and uncertified contacts with whom the user is attempting to communicate;~~ and

~~(c)~~(d) warning the user and restricting the user from communicating with the selected contact based on the security policy when the selected contact has ~~contacts with~~ an unauthenticated and uncertified level.

15. (Original) The method of claim 14 wherein step (a) comprises a user setting the security policy that applies to that user.

16. (Original) The method of claim 14 wherein step (a) comprises a system administrator setting a security policy that applies to a user.

17. (Currently Amended) The method of claim 14 wherein step ~~(c)~~(d) comprises warning a user when the security policy is set to warn and the user attempts to communicate with an unauthenticated and uncertified contact.

18. (Currently Amended) The method of claim 14 wherein step ~~(c)~~(d) comprises preventing a user from communicating with an uncertified contact when the security policy is set to restrict and the user attempts to communicate with an uncertified contact.

19. (Currently Amended) The method of claim 14 wherein step ~~(c)~~(d) comprises allowing a user to communicate with an unauthenticated and uncertified contact when the security policy is set to allow without warning and the user attempts to communicate with an unauthenticated and uncertified contact.

20. (Currently Amended) The method of claim 14 wherein step ~~(b)~~(c) comprises:

~~(b1)~~(c1) compiling a contact list of contacts with whom the user is attempting to communicate;

~~(b2)~~(c1) checking the contact list to determine contacts that are not authenticated;

~~(b3)~~(c3) checking the unauthenticated contacts to determine whether a certification policy applies to any unauthenticated contact; and

~~(b4)~~(c4) placing an unauthenticated contact on the list of unauthenticated and uncertified contacts when no certification policy applies to that contact.

21. (Currently amended) Apparatus for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple identities each with an associated display name, comprising:

means for displaying on a graphic user interface, a name conflict indicator next to a first ~~and a second~~ display name~~, which display names are~~ that is associated with a first identity, the first identity being different than at least one second identity associated with at least one second display name, the at least one second display name being ~~identities and are~~ equivalent to the first display name;

means responsive to user input associated ~~a selection of a display name~~ with ~~a~~ the name conflict indicator~~displayed next thereto~~ for displaying a plurality of ~~all~~ display names that are equivalent to the ~~selected~~ first display name;

means for receiving user input specifying an alternative display name for a selected display name of the plurality of equivalent display names, the selected display name being associated with a selected identity and being different than the first display name; and

means for identifying on a second graphic user interface the selected identity with the alternative display name, the graphic user interface providing a function related to controlling communication within the peer-to-peer collaboration system ~~a mechanism that resolves the name conflict between two conflicting display names~~.

22. (Original) The apparatus of claim 21 wherein the means for displaying a name conflict indicator comprises a mechanism that computes a clean name from each display name and a comparator that compares the clean names of two display names to determine if the two display names are equivalent.

23. (Original) The apparatus of claim 21 wherein each contact identity has an authentication level associated therewith and wherein the means for displaying a name conflict indicator comprises:

means for examining the authentication levels of all display names that are equivalent; and

means for displaying name conflict indicators next to selected display names based on display names that are determined to be equivalent by the means for examining the authentication levels.

24. (Original) The apparatus of claim 23 wherein the means for displaying name conflict indicators next to selected display names comprises means for displaying a name conflict indicator next to each display name associated with a contact identity whose authentication level (1) is less than the highest authentication/certification level of all contact identities with equivalent display names or (2) equals the highest authentication/certification level to which at least two contact identities with equivalent display names have equal authentication levels.

25. (Original) The apparatus of claims 23 further comprising:

a mechanism that provides a security policy that determines the behavior of the collaboration system regarding communications with a contact based on the authentication level of that contact.

26. (Original) The apparatus of claim 25 wherein a mechanism that provides the security policy comprises a mechanism that allows a user of the collaboration system to determine the security policy.

27. (Original) The apparatus of claim 25 wherein the mechanism that provides the security policy comprises a mechanism that allows a system administrator to determine the security policy.

28. (Original) The apparatus of claim 25 further comprising:

a mechanism that warns a user based on the security policy when that user attempts to communicate with a contact having a predetermined authentication level.

29. (Original) The apparatus of claim 25 further comprising:

a mechanism that prevents a user from communicating with another user based on the security policy when the other user has a predetermined authentication level.

30. (Original) The apparatus of claim 21 wherein the means for displaying all display names that are equivalent to the selected display name comprises means for displaying a dialog box having all display names that are equivalent to the selected display name listed therein.

31. (Original) The apparatus of claim 21 wherein the a mechanism that resolves the name conflict comprises a mechanism for assigning an alias to one of the first and

second display names which alias is not equivalent to either of the first and second display names and which alias replaces the one display name.

32. (Original) The apparatus of claim 21 further comprising:

a mechanism that displays an authentication indicator next to a display name that is not equivalent to another display name, which authentication indicator displays the authentication level of the associated contact.

33. (Original) The apparatus of claim 32 wherein each contact can have one of a predetermined number of authentication levels and wherein the authentication indicator that is displayed is unique to one of the authentication levels.

34. (Currently amended) Apparatus for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple authentication and certification levels, including an unauthenticated and uncertified level, comprising:

a mechanism that sets a security policy that controls the behavior of the collaboration system based on the authentication and certification level;

means for receiving through a graphic user interface an indication of a selected contact with which to communicate;

means for obtaining the authentication and certification level of the selected contact;

~~means responsive to an attempt by a user to communicate with one or more contacts for compiling a list of unauthenticated and uncertified contacts with whom the user is attempting to communicate;~~ and

a mechanism that warns the user and restricts the user from communicating with the selected contact based on the security policy when the selected contact has ~~contacts with~~ an unauthenticated and uncertified level based on the security policy.

35. (Original) The apparatus of claim 34 wherein the mechanism that sets the security policy comprises a mechanism that allows a user to set the security policy that applies to that user.

36. (Original) The apparatus of claim 34 wherein the mechanism that sets the security policy comprises a mechanism that allows a system administrator to set a security policy that applies to a user.

37. (Original) The apparatus of claim 34 wherein the mechanism that warns the user and restricts the user comprises a mechanism that warns a user when the security policy is set to warn and the user attempts to communicate with an unauthenticated and uncertified contact.

38. (Original) The apparatus of claim 34 wherein the mechanism that warns the user and restricts the user comprises a mechanism that prevents a user from communicating with an uncertified contact when the security policy is set to restrict and the user attempts to communicate with an uncertified contact.

39. (Original) The apparatus of claim 34 wherein the mechanism that warns the user and restricts the user comprises a mechanism that allows a user to communicate with an unauthenticated and uncertified contact when the security policy is set to allow without warning and the user attempts to communicate with an unauthenticated and uncertified contact.

40. (Currently amended) The apparatus of claim 34 wherein the means for obtaining the authentication and certification level ~~compiling a list of unauthenticated and uncertified contacts~~ comprises:

means for compiling a contact list of contacts with whom the user is attempting to communicate;

means for checking the contact list to determine contacts that are not authenticated;

means for checking the unauthenticated contacts to determine whether a certification policy applies to any unauthenticated contact; and

means for placing an unauthenticated contact on the list of unauthenticated and uncertified contacts when no certification policy applies to that contact.

41. (Original) A computer program product for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple identities each with an associated display name, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code for displaying on a graphic user interface a name conflict indicator next to a first ~~and a second~~ display name~~, which display names are~~ that is associated with a first identity different than at least one second identity associated with at least one second display name, the at least one second display name being ~~identities and are~~ equivalent to the first display name;

program code operable in response to user input associated ~~a selection of a display name~~ with ~~a~~ the name conflict indicator~~displayed next thereto,~~ for displaying a plurality of ~~all~~ display names that are equivalent to the ~~selected~~ first display name; ~~and~~

program code for receiving user input specifying an alternative display name for a selected display name of the plurality of equivalent display names, the selected display name being associated with a selected identity and being different than the first display name; and

program code for identifying on a second graphic user interface the selected identity with the alternative display name, the graphic user interface providing a function related to

controlling communication within the peer-to-peer collaboration system ~~that provides a mechanism to resolve the name conflict between two conflicting display names~~.

42. (Currently amended) A computer program product for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple authentication and certification levels, including an unauthenticated and uncertified level, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code for setting a security policy that controls the behavior of the collaboration system based on the authentication and certification level;

program code for receiving through a graphic user interface an indication of a selected contact with which to communicate;

program code for obtaining the authentication and certification level of the selected contact ~~operable in response to an attempt by a user to communicate with one or more contacts, for compiling a list of unauthenticated and uncertified contacts with whom the user is attempting to communicate~~; and

program code for warning the user and restricting the user from communicating with the selected contact based on the security policy when the selected contact has ~~contacts with~~ an unauthenticated and uncertified level based on the security policy.